CLAIMS

1. A method for improving the security of a counter mode block cipher that breaks a message into text bytes and encrypts each text byte with a fixed, secret key with a keysize, the method comprising:

(a) generating a random byte sequence for each message;

(b) combining the random byte sequence with the key to form a modified key; and

(c) conveying the modified key to the block cipher so that each text byte is encrypted with the modified key.

2. The method of claim 1 wherein the random byte sequence has same size as the keysize and step (b) comprises combining the random byte sequence with the key with a bitwise exclusive-OR function.

3. The method of claim 1 wherein step (b) comprises concatenating the random byte sequence with the key and passing the concatenation through a mask generation function to obtain the modified key.

4. The method of claim 1 wherein the random byte sequence is non-secret.

5. The method of claim 1 wherein the mask generation function is a one-way function.

6. Apparatus for improving the security of a counter mode block cipher that breaks a message into text bytes and uses an encryption algorithm to encrypt each text byte with a fixed, secret key with a keysize, the apparatus comprising:

a sequence generator that generates a random byte sequence for each message;

a key generator that combines the random byte sequence with the key to form a modified key; and

a mechanism that conveys the modified key to the encryption algorithm so that each text byte is encrypted with the modified key.

7. The apparatus of claim 6 wherein the random byte sequence has same size as the keysize and the key generator comprises a bitwise exclusive-OR function that combines the random byte sequence with the key.

8. The apparatus of claim 6 wherein the key generator comprises a mechanism that concatenates the random byte sequence with the key and a mask generation function that operates on the concatenation to obtain the modified key.

9. The apparatus of claim 6 wherein the random byte sequence is non-secret.

10. The apparatus of claim 6 wherein the mask generation function is a one-way function.

11. A method for improving the security of a stream cipher that encrypts a continuous byte stream of messages with a fixed, secret key with a keysize, the method comprising:

(a) generating a random byte sequence for each message;

(b) combining the random byte sequence with the key to form a modified key; and

(c) conveying the modified key to the stream cipher so that each message stream is encrypted with the modified key.

12. The method of claim 11 wherein the random byte sequence has same size as the keysize and step (b) comprises combining the random byte sequence with the key with a bitwise exclusive-OR function.

13. The method of claim 11 wherein step (b) comprises concatenating the random byte sequence with the key and passing the concatenation through a mask generation function to obtain the modified key.

14. The method of claim 11 wherein the random byte sequence is non-secret.

15. The method of claim 11 wherein the mask generation function is a one-way function.

16. Apparatus for improving the security of a stream cipher that encrypts a continuous byte stream of messages with a fixed, secret key with a keysize, the apparatus comprising:

a sequence generator that generates a random byte sequence for each message;

a key generator that combines the random byte sequence with the key to form a modified key; and

a mechanism that conveys the modified key to the encryption algorithm so that each message stream is encrypted with the modified key.

17. The apparatus of claim 16 wherein the random byte sequence has same size as the keysize and the key generator comprises a bitwise exclusive-OR function that combines the random byte sequence with the key.

18. The apparatus of claim 16 wherein the key generator comprises a mechanism that concatenates the random byte sequence with the key and a mask generation function that operates on the concatenation to obtain the modified key.

19. The apparatus of claim 16 wherein the random byte sequence is non-secret.

20. The apparatus of claim 16 wherein the mask generation function is a one-way function.

21. A computer program product for improving the security of a stream cipher that encrypts a continuous byte stream of messages with a fixed, secret key with a keysize, the computer program product comprising a computer usable medium having computer readable code thereon, including:

program code that generates a random byte sequence for each message;

program code that combines the random byte sequence with the key to form a modified key; and

program code that conveys the modified key to the stream cipher so that each message stream is encrypted with the modified key.

22. The computer program product of claim 21 wherein the random byte sequence has same size as the keysize and the program code that generates a random byte sequence comprises program code that combines the random byte sequence with the key with a bitwise exclusive-OR function.

23. The computer program product of claim 21 wherein the program code that generates a random byte sequence comprises program code that concatenates the random byte sequence with the key and passes the concatenation through a mask generation function to obtain the modified key.

24. The computer program product of claim 21 wherein the random byte sequence is non-secret.

25. The computer program product of claim 21 wherein the mask generation function is a one-way function.

26. A computer program product for improving the security of a counter mode block cipher that breaks a message into text bytes and uses an encryption algorithm to encrypt each text byte with a fixed, secret key with a keysize, the computer program product comprising a computer usable medium having computer readable code thereon, including:

program code that generates a random byte sequence for each message;

program code that combines the random byte sequence with the key to form a modified key; and

program code that conveys the modified key to the block cipher so that each text byte is encrypted with the modified key.

27. The computer program product of claim 26 wherein the random byte sequence has same size as the keysize and the program code that generates a random byte sequence comprises program code that combines the random byte sequence with the key with a bitwise exclusive-OR function.

28. The computer program product of claim 26 wherein the program code that generates a random byte sequence comprises program code that concatenates the random byte sequence with the key and passes the concatenation through a mask generation function to obtain the modified key.

29. The computer program product of claim 26 wherein the random byte sequence is non-secret.

30. The computer program product of claim 26 wherein the mask generation function is a one-way function.

31. A computer data signal embodied in a carrier wave for improving the security of a stream cipher that encrypts a continuous byte stream of messages with a fixed, secret key with a keysize, the computer data signal comprising:

program code that generates a random byte sequence for each message;

program code that combines the random byte sequence with the key to form a modified key; and

program code that conveys the modified key to the stream cipher so that each message stream is encrypted with the modified key.

32. A computer data signal for improving the security of a counter mode block cipher that breaks a message into text bytes and uses an encryption algorithm to encrypt each text byte with a fixed, secret key with a keysize, the computer data signal comprising:

program code that generates a random byte sequence for each message;

program code that combines the random byte sequence with the key to form a modified key; and

program code that conveys the modified key to the block cipher so that each text byte is encrypted with the modified key.